# National Infrastructure Protection Center CyberNotes

*Issue #2002-21* *October 21, 2002*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between October 1 and between October 17, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Andrew G. Morgan[1] | Unix | Linux PAM 0.76 | A vulnerability exists in PAM due to the way locked passwords are treated, which could let an unauthorized remote malicious user obtain access to target systems. | Upgrade available at:<br>http://ftp.debian.org/debian/pool/main/p/pam/ |

[1] Debian Security Advisory, DSA 177-1, October 17, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Apache Software Foundation[2] | Unix | Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17- 1.3.19, 1.3.20, 1.3.22- 1.3.27 | Multiple vulnerabilities exist: several buffer overflow vulnerabilities exist in the 'htdigest' utility due to improper bounds checking when user-supplied data is copied into local buffers, which could possibly let a malicious user execute arbitrary code; a vulnerability exists in the 'htdigest' utility due to insecure system() calls when commandline options are processed, which could let a malicious user execute arbitrary code; and a vulnerability exists because 'htpasswd' temporary files are created insecurely, which could let a malicious user read or corrupt the Apache password file and possibly obtain unauthorized access. | No workaround or patch available at time of publishing. |
| ArGoSoft[3] | Windows 95/98/NT 4.0/2000, XP | Mail Server Pro 1.8.1 .9 | A Cross-Site Scripting vulnerability exists because HTML in e-mail messages is not sufficiently sanitized, which could let a remote malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. |
| Authoria[4] | Windows 2000, Unix | HR Suite | A Cross-Site Scripting vulnerability exists in 'AthCGI.EXE' due to inadequate URL filtering, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. |

[2] Bugtraq, October 16, 2002.
[3] Bugtraq, October 7, 2002.
[4] SecurityTracker Alert ID 1005401, October 10, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Avaya[5] | Multiple | Cajun P550 Series Fireware 4.3.5, P550R Series Firmware 5.2.14, P580 Series Firmware 5.2.14,<br>P880 Series Firmware 5.2.14, P882 Series Firmware 5.2.14 | A vulnerability exists because two undocumented accounts exist that allow access via Telnet and web interface and have default passwords, which could let a remote unauthorized malicious user obtain privileged access to the switch and modify arbitrary configuration settings. | Upgrade available at:<br>http://support.avaya.com |
| Balabit[6, 7] | Unix | syslog-ng 1.4 .0rc3, 1.4.7-1.4.10, 1.4.15, 1.5.15, 1.5.20 | A buffer overflow vulnerability exists because the syslog-ng macro expansion fails to do proper bounds checking when handling constant characters, which could let a remote malicious user execute arbitrary commands. | **Debian:**<br>http://security.debian.org/pool/updates/main/s/syslog-ng/<br>**Engarde:**<br>ftp://ftp.engardelinux.org/pub/engarde/stable/updates/<br>**Balabit:**<br>http://www.balabit.hu/en/downloads/syslog-ng/downloads/ |
| BEA Systems, Inc.[8] | Multiple | WebLogic Express 7.0 SP 1, WebLogic Integration 7.0, 7.0SP1, WebLogic Platform 7.0 SP 1, Weblogic Server 7.0 SP 1 | A vulnerability exists because undocumented extensions are supported for the Servlet 2.3 specification and are no longer supported in recent versions, which could cause web applications to run without security policies being enforced. | **WebLogic Server 7.0 SP 1 Workaround:**<br>Vendor advises users to edit web.xml files which use the extended URL pattern s appropriate entries are prefixed with a '/' character.<br>**BEA Systems Weblogic Server 7.0 SP 1:**<br>ftp://ftpna.beasys.com/pub/releases/security/CR086158_70sp1.jar<br>**BEA Systems WebLogic Express 7.0 SP 1, WebLogic Integration 7.0 SP 1, W Platform 7.0 SP 1:**<br>ftp://ftpna.beasys.com/pub/releases/security/CR087623_70SP1.zip |
| Check Point Software Technologies[9] | Multiple | VPN-1 4.1, 4.1 SP1-SP4 | A vulnerability exists due to the failure to properly respond to Internet Key Exchange (IKE) Aggressive Mode session requests, which could let a remote malicious user bypass security restrictions. | A hotfix is available through the Check Point site (login required). Information av<br>http://www.checkpoint.com/techsupport/alerts/ike.html |
| Cisco Systems[10] | Multiple | Unity Server 2.0-2.4, 2.46, 3.0, 3.1 | A vulnerability exists because predefined restriction tables do not block calls to the international operator, which could let a malicious user circumvent International Direct Dial restrictions. | Workaround available at:<br>http://www.cisco.com/warp/public/707/toll-fraud-pub.shtml |

[5] Securiteam, October 17, 2002.
[6] Debian Security Advisory, DSA 175-1, October 15, 2002.
[7] EnGarde Secure Linux Security Advisory, ESA-20021016-025, October 16, 2002.
[8] BEA Systems Security Advisory, BEA02-22.00, October 15, 2002.
[9] CheckPoint Security Alert, October 7, 2002.
[10] Cisco Security Advisory Revision 1.1, October 5, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Cisco Systems[11] | Multiple | CatOS 5.4, 5.5 (13a), 5.5, 6.1 (2), 6.1, 7.3, 7.4 | A remote Denial of Service vulnerability exists in versions of CatOS that contain a "cv" in the image name due to a buffer overflow condition in the HTTP server when an overly long HTTP query is received. | Upgrade available at:<br>http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml |
| Citrix[12] | Windows 2000 | MetaFrame XPs, XPe, XPa, XP, MetaFrame | A vulnerability exists when a specially crafted request is sent to the server and the responses are examined, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| Click2 Learn[13] | Multiple | Ingenium Learning Manage-ment System 5.1, 6.1 | Multiple vulnerabilities exist: a vulnerability exists in the default installation because password information is left in a directory that is publicly accessible via the web, which could let a malicious user obtain sensitive information; and a vulnerability exists because a weak algorithm is used to hash user and administrative credentials, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| Cool Forum[14] | Unix | CoolForum 0.5 beta | A vulnerability exists in the 'avatar.php' script when maliciously constructed requests are sent, which could let a remote malicious user obtain sensitive information. | Upgrade available at:<br>http://www.coolforum.net/index.php?p=dlcoolforumc |
| Cooolsoft[15] | Windows 95/98/ME/ NT 4.0/2000, XP | PowerFTP 2.0 3, 2.10, 2.23, 2.24 | A remote Denial of Service vulnerability exists because long user names are not properly handled. | No workaround or patch available at time of publishing. |

[11] Cisco Security Advisory, 20021016, October 16, 2002.
[12] Bugtraq, October 2, 2002.
[13] Bugtraq, October 14, 2002.
[14] Securiteam, October 17, 2002.
[15] Bugtraq, October 5, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Ekilat LLC[16] | Unix | php (Reactor) 1.2.7 pl1 | A Cross-Site Scripting vulnerability exists in 'Browse.PHP,' which could let a malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. |
| Francisco Burzi[17] | Windows, Unix | PHP-Nuke 6.0 | Multiple Cross-Site Scripting vulnerabilities exist in various features, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. |
| Free Peers, Inc.[18] | Windows 95/98/ME/ NT 4.0/2000, XP | BearShare 2.2-2.2.3, 4.0-4.0.2, 4.0.4-4.0.6 | A Directory Traversal vulnerability exists due to improper input validation, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| GazTek[19] | Unix | ghttpd 1.4-1.4.3 | A buffer overflow vulnerability exists in the Log() function when the GET request argument is excessively long, which could let a remote malicious user execute arbitrary code. | Patch available at:<br>http://lynorics.sundawn.net/prog/ghttpd-1.4-3.diff |
| Hewlett Packard Systems[20] | Unix | OnlineJFS 3.1 | A vulnerability exists because standard UNIX filesystem security measures are not being observed in the JournalFS.VXFS-VASE-KRN fileset when OnLineJFS is being used, which could let an unauthorized malicious user modify properties of sensitive files. | Patches available at:<br>http://itrc.hp.com<br>Patch PHKL_24201, Patch PHKL_27833, Patch PHKL_27832 |
| Hewlett Packard Systems, Inc.[21] | Unix | Compaq Tru64 4.0 g PK3 (BL17), 4.0f PK7 (BL18), 5.0a PK3 (BL17), 5.1a PK3 (BL3), 5.1 PK5 (BL19) | A vulnerability exists in the route daemon (routed), which could let a remote malicious user obtain unauthorized access. | Patches available at:<br>http://ftp.support.compaq.com/patches/public/unix/ |

[16] Bugtraq, October 10, 2002.
[17] Bugtraq, October 10, 2002.
[18] Securiteam October 1, 2002.
[19] Securiteam, October 15, 2002.
[20] Hewlett Packard Systems Security Advisory, HPSBUX0210-223, October 16, 2002.
[21] Hewlett Packard Systems Security Bulletin, SSRT2208, October 7, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| IBM[22] | Multiple | SecureWay Firewall 4.2, 4.2.1 | A remote Denial of Service vulnerability exists in the stack implementation when processing TCP packets that contain zero bit flags. | Update available at:<br>ftp://testcase.software.ibm.com/aix/fromibm/firewall/fwaixfilter4_421d.tar |
| IBM[23] | Unix | AIX 4.3.3, 5.1 | A remote Denial of Service vulnerability exists when a malicious user sends malformed TCP packets that have all of the flags set to zero. | No workaround or patch available at time of publishing. |
| KDE[24] | Unix | KDE 3.0.1-3.0.3 | A vulnerability exists in the 'kpf' file sharing utility, which could let a remote malicious user obtain sensitive information. | Upgrade available at:<br>http://download.kde.org/stable/3.0.4 |
| Killer Protection[25] | Multiple | Killer Protection 1.0 | A vulnerability exists in the 'php' script, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| Logsurfer[26] | Windows, Unix | Logsurfer 1.5 a, 1.5, 1.41 | Two vulnerabilities exist: a buffer overflow vulnerability exists due to an off-by-one error in the' context_action()' function, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exists in the 'eadcfg()' function due to improperly initialization, which could let a remote malicious user | Upgrade available at:<br>ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/ |
| Macro-media[27] | Multiple | Flash 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0 | A vulnerability exists due to an error when animations are loaded from remote SMB shares in the Flash Player, which could let a remote malicious user read the contents of local files through Flash Player's XML control. | No workaround or patch available at time of publishing. |

[22] Securiteam, October 1, 2002.
[23] Bugtraq, October 9, 2002.
[24] KDE Security Advisory, October 8, 2002.
[25] SecurityTracker Alert ID 1005376, October 8, 2002.
[26] Bugtraq, October 4, 2002.
[27] Bugtraq, October 7, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| **Microsoft[28]**<br>***Microsoft issues bulletin[29]*** | **Windows 95/98/ME/ NT 4.0/2000, XP, MacOS** | **Word 2000, 2000 SR1a, 2000 SR1&2, Word 2002, Word 95, Word 97, 97 SR1&2, Word 98, *Word 2001 for Macintosh Word 98 for Macintosh, Word 98 Japanese Version, Excel 2002*** | **A vulnerability exists when the INCLUDETEXT Field Code references a file on the local system and is included in a document, which could let a malicious user insert an arbitrary local file into a document.** | ***Frequently asked questions regarding this vulnerability and the patch can be fo*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security 059.asp** |
| Microsoft[30] | Windows 95/98/NT 4.0/2000, XP | TSAC ActiveX Control | A Cross-Site Scripting vulnerability exists in the 'connect.asp' file because external input is not properly sanitized, which could let a remote malicious user execute arbitrary HTML and script code. | Upgrade available at:<br>http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp |
| Microsoft[31] | Windows NT 4.0/2000, XP | Content Management Server 2001, 2001 SP1 | A Cross-Site Scripting vulnerability exists because the 'ManualLogin.asp' script does not filter user-supplied HTML from the 'REASONTXT' parameter, which could let a remote malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. |
| Microsoft[32] | Windows XP | Windows XP Profes-sional | A vulnerability exists in the "System Restore" directory and subdirectories due to insecure access permissions, which could let an unauthorized malicious user obtain sensitive information. | Windows XP Service Pack 1 available at:<br>http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp |

[28] Bugtraq, August 26, 2002.
[29] Microsoft Security Bulletin, MS02-059 V1.1, October 17, 2002.
[30] SNS Advisory No.56, October 11, 2002.
[31] Bugtraq, October 7, 2002.
[32] Bugtraq, October 4, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Microsoft[33] | Windows 2000, XP | Windows 2000 Advanced Server, Advanced Server SP1&2, 2000 Datacenter Server, Datacenter Server SP1&2, 2000 Profes-sional, Profes-sional SP1&2, 2000 Server, 2000 Server SP1&2, 2000 Terminal Services, Terminal Services SP1&2, XP Home, XP Profes-sional | A security vulnerability exists if the option 'Do not overwrite events (clear log manually)' is selected and the Event Log has reached the maximum size which will cause administrative alerts not to be sent. | This issue was addressed in Windows 2000 service pack 3 and Windows XP servi available at:<br>http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/sp3lang.asp<br>http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp |
| Microsoft[34] | Windows 2000, XP | IIS 5.0, 5.1 | A remote Denial of Service vulnerability exists when a malicious user sends a HTTP request for 'shtml.dll' that contains a malformed HOST field. | No workaround or patch available at time of publishing. |
| Microsoft[35] | Windows 2000 | IIS 5.0 | A Cross-Site Scripting vulnerability exists when a request contains a long URL and ends in the .idc extension, which could let a malicious user execute arbitrary script code. | No workaround or patch available at time of publishing. |
| Microsoft[36] | Windows 95/98/ME NT 4.0/2000 | Internet Explorer 5.5, 5.5 SP1&2, 6.0 | A vulnerability exists because adequate access control checks are not performed on all frame properties, which could let a malicious user obtain unauthorized access. | This issue is reportedly addressed in Microsoft Internet Explorer 6.0 SP1. Users ar upgrade. |

[33] Securiteam, October 17, 2002.
[34] Bugtraq, October 7, 2002.
[35] SecurityFocus, October 5, 2002.
[36] GreyMagic Security Advisory, GM#011-IE, October 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Microsoft[37] | Windows 2000 | Windows 2000 Terminal Services, Terminal Services SP1-SP3, 2000 Server, Server SP1-SP3, 2000 Profes-sional, Profes-sional SP1-SP3, 2000 Datacenter Server, Datacenter Server SP1-SP3, 2000 Advanced Server, Advanced Server SP1-SP3 | A vulnerability exists in the Winlogon NetDDE Agent, which could let a malicious user obtain elevated privileges. | No workaround or patch available at time of publishing. |
| Microsoft[38] | Windows 95/98/NT 4.0/2000, XP | Outlook Express 5.5, 6.0 | A buffer overflow vulnerability exists in the code that generates warning messages when certain error conditions associated with digital signatures are encountered, which could let a malicious user execute arbitrary code. | Frequently asked questions regarding this vulnerability and the patch can be found<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02 |
| **Microsoft[39]**<br>***Microsoft issues bulletin[40]*** | **Windows XP** | **Windows XP Home, XP Profes-sional, Internet Explorer 6.0** | **A vulnerability exists in the Microsoft Help and Support Center HCP URI handler, which could let a remote malicious user delete files on another user's computer.** | ***Frequently asked questions regarding this vulnerability and the patch can be fo***<br>**http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security**<br>**060.asp** |

[37] Security Advisory 10.06.2002, October 9, 2002.
[38] Microsoft Security Bulletin, MS02-058 V1.2, October 11, 2002.
[39] Bugtraq, August 15, 2002.
[40] Microsoft Security Bulletin, MS02-060 V1.1, October 17, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Microsoft[41] | Windows NT 4.0/2000 | Data Engine 1.0, 2000, SQL Server 7.0, SQL Server 7.0 SP1-SP4, SQL Server 2000, SQL Server 2000 SP1&2, | A vulnerability exists because there is a flaw in the stored procedure that runs web tasks due to the way permissions are handled, which could let a malicious user obtain elevated privileges. In addition, there are weak permissions on the web tasks table that together with the stored procedure could allow a malicious user to run, delete or update a web task.<br>*Note: This patch supersedes the one provided in Microsoft Security Bulletin MS02-056, which was also a cumulative patch.* | Frequently asked questions regarding this vulnerability and the patch can be foun<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02<br>*Note: This is a cumulative patch that includes the functionality of all previously re for SQL Server 7.0, SQL Server 2000, and Microsoft Data Engine (MSDE) 1.0, M Engine (MSDE) 2000. In addition, it eliminates one newly discovered vulnerabilit* |
| Mondo Soft, Inc.[42] | Windows | Mondo Search 4.4 | A vulnerability exists when a remote malicious user sends a specially crafted URL request for a known file, which could let a malicious user obtain the file's source code. | No workaround or patch available at time of publishing. |
| Multiple Vendors[43, 44] | Unix | Linux-HA heartbeat 9.4.9.1, 0.4.9a<br>-0.4.9c, 0.9.4 d | A buffer overflow vulnerability exists due to the way TCP packets are handled, which could let a remote malicious user execute arbitrary code. | The vulnerability is eliminated in versions 0.4.9.2 and 0.4.9e available at:<br>http://linux-ha.org/download/<br>**SuSE:**<br>ftp://ftp.suse.com/pub/suse/i386/update/8.0/<br>**Debian:**<br>http://security.debian.org/pool/updates/main/h/heartbeat/ |

[41] Microsoft Security Bulletin, MS02-061, October 16, 2002.
[42] Bugtraq, October 10, 2002.
[43] SuSE Security Announcement, SuSE-SA:2002:037, October 14, 2002.
[44] Debian Security Advisory, DSA 174-1, October 14, 2002

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Multiple Vendors[45] | Windows 98/98/ME/ NT 4.0/2000, XP | Internet Security Systems BlackICE Defender 2.9 cap, BlackIce Server Protection 3.5 cdf;<br>Symantec Norton Personal Firewall 2002 | A remote Denial of Service vulnerability exists due to the way spoofed traffic is handled. | No workaround or patch available at time of publishing. |
| Multiple Vendors[46, 47] | Unix | Linux kernel 2.4.1- 2.4.18 | Multiple vulnerabilities exist: a vulnerability exists in the BTTY video capture card driver, which could let a malicious user obtain elevated privileges and possibly cause a Denial of Service; a vulnerability exists in the PCILynx FireWire driver, which could let a malicious user obtain elevated privileges and possibly cause a Denial of Service; and a Denial of Service vulnerability exists in the IXJ telephony card driver. | **RedHat:** ftp://updates.redhat.com/ |
| Multiple Vendors[48, 49] | Unix | Linux kernel 2.2.1- 2.2.21 | Numerous security vulnerabilities exist which could let a malicious user obtain elevated (root) privileges. | Upgrade to Linux 2.2.22 kernel.<br>**RedHat:**<br>ftp://updates.redhat.com/<br>**Trustix:**<br>ftp://ftp.trustix.net/pub/Trustix/updates/ |
| Multiple Vendors[50, 51] | Unix | Hewlett Packard Secure OS software for Linux 1.0;<br>RedHat Linux 6.2, 6.2 sparc, i386, alpha,7.0, 7.0 i386, alpha, 7.1, 7.1 ia64, i386, alpha, 7.2, 7.2 ia64, i386, 7.3, 7.3 i386, 8.0, 8.0 i386 | A vulnerability exists in 'dvips' when a maliciously constructed file is passed to the lpd daemon, which could let a malicious user execute arbitrary commands. | Updates available at:<br>ftp://updates.redhat.com/ |

[45] Bugtraq, October 10, 2002.
[46] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:206-12, October 15, 2002.
[47] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:205-15, October 17, 2002.
[48] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:210-06, October 17, 2002.
[49] Trustix Secure Linux Security Advisory, TSLSA-2002-0068, October 17, 2002.
[50] Hewlett Packard Systems Security Bulletin, HPSBTL0210-073, October 15, 2002.
[51] RedHat Security Advisory, RHSA-2002:194-18, October 10, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Multiple Vendors[52] | Unix | Compaq Tru64 4.0 g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f, 5.0 a PK3 (BL17), 5.0a, 5.1 a PK3 (BL3), 5.1a, 5.1 PK5 (BL19), 5.1; Hewlett Packard Systems HP-UX 10.20, 11.0, 11.11, 11.22 | A vulnerability exists in the 'ypserv' daemon, which could let a local/remote malicious user obtain unauthorized access to sensitive information. | **Compaq:**<br>http://ftp.support.compaq.com/patches/public/unix/ |
| **Multiple Vendors[53][54]**<br>***More patches released*[55, 56, 57, 58, 59]** | **Windows NT 4.0/2000, Unix** | **Apache Software Founda-tion Apache 1.3.20, 1.3.22- 1.3.26; Oracle Internet Application Server 1.0.2.1, 1.0.2.0, 8i Enterprise Edition 8.1.7.1.0, 8.1.7.0.0, 9i Application Server, 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2, 9.0.2 release 2, 9iAS Reports 9.0.2 .1, Oracle8 8.1.7, 8.1.7.1, 8.1.7, Oracle9i Release 2 9.2 .2, 9.0.2** | **Multiple vulnerabilities exist: a Denial of Service vulnerability exists due to the way the Apache scorecare is handled; a Cross-Site Scripting vulnerability exists due to improper santization of SSI error pages, which could let a malicious user execute arbitrary HTML or JavaScript code; and a buffer overflow vulnerability exists in the ab.c web benchmarking support utility, which could let a malicious user execute arbitrary code.** | **Apache Software Foundation:**<br>**http://www.apache.org/dist/httpd/apache_1.3.27.tar.gz**<br>**Oracle Corporation:**<br>**Oracle has stated that fixes for affected software will be available October 8,**<br>**metalink.**<br>**OpenPKG:**<br>**ftp://ftp.openpkg.org/release/1.0/UPD/**<br>***Engarde Secure Linux:***<br>**ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/apache-1.3.27-1.0.32.i386.r**<br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/ftp.php**<br>*FreeBSD:*<br>**ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/**<br>*Oracle:*<br>**http://metalink.oracle.com**<br>***Trustix:***<br>http://www.trustix.net/pub/Trustix/updates/ |

[52] Hewlett Packard Systems Security Bulletin, SSRT2368, October 7, 2002.
[53] iDEFENSE Security Advisor, 10.03.2002, October 3, 2002.
[54] OpenPKG Security Advisory, OpenPKG-SA-2002.009, October 4, 2002.
[55] EnGarde Secure Linux Security Advisory, ESA-20021007-024, October 7, 2002.
[56] FreeBSD Security Notice, FreeBSD-SN-02:06, October 10, 2002.
[57] Mandrake Linux Security Update Advisory, MDKSA-2002:068, October 16, 2002.
[58] Oracle Security Alert #45, October 4, 2002.
[59] Trustix Secure Linux Security Advisory, 2002-0069, October 17, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Multiple Vendors[60, 61, 62, 63] | Unix | Compaq Tru64 4.0 g PK3 (BL17), 4.0g, 4.0 f PK7 (BL18), 4.0f, 5.0 a PK3 (BL17), 5.0a, 5.1 a PK3 (BL3), 5.1a, 5.1 PK5 (BL19), 5.1;<br>HP HP-UX 10.20, 11.0, 11.11, 11.22;<br>Caldera OpenLinux 2.2-2.4;<br>SCO OpenServer 5.0.5, 5.0.6; Sun Micro-systems, Inc. Solaris 2.6, 7, 8, and 9;<br>IBM AIX 4.3.3, 5.0.1 | A vulnerability exists in the 'ypxfrd' daemon due to improper arguments validation, which could let a local/remote malicious user obtain sensitive information. | **Compaq:**<br>http://ftp.support.compaq.com/patches/public/unix/<br>**SCO OpenServer:**<br>ftp://ftp.caldera.com/pub/updates/OpenServer/CSSA-2002-SCO.40<br>**Sun Microsystems:**<br>http://sunsolve.sun.com/securitypatch<br>**IBM:**<br>ftp://ftp.software.ibm.com/aix/efixes/security/ypserv_efix.tar.Z |
| myPHP Nuke[64] | Multiple | myPHP Nuke 1.8.8 | A vulnerability exists in the 'phptonuke.php' file when malicious requests are passed to the webserver due to insufficient santization of user-supplied input, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| MyWeb Server[65] | Windows 95/98/ME/ NT 4.0/2000 | MyWeb Server 1.0.0-1.0.2 | A remote Denial of Service vulnerability exists when a malicious user submits a unusually long HTTP GET request. | No workaround or patch available at time of publishing. |
| NetBSD[66] | Unix | NetBSD 1.5-1.5.3, 1.6 | A buffer overflow vulnerability exists in the 'talkd' service due to improper bounds checking on inbound messages, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code. | Information and upgrade available at: http://lists.netsys.com/pipermail/full-disclosure/2 October/002406.html |

[60] Hewlett Packard Systems Security Bulletin, SSRT2339, October 7, 2002.
[61] SCO Security Advisory, CSSA-2002-SCO.40, October 10, 2002.
[62] Sun(sm) Alert Notification 47903, October 15, 2002.
[63] IBM Alert, October 11, 2002.
[64] Bugtraq, October 16, 2002.
[65] Securiteam, October 15, 2002.
[66] NetBSD Security Advisory, 2002-019, October 8, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Netgear[67] | Multiple | FM114P Wireless Firewall | A remote Denial of Service vulnerability when a malicious user makes an unusually large number of TCP connections or trying to brute force the password used in the administrator's web interface. | No workaround or patch available at time of publishing. |
| Netgear[68] | Multiple | FM114P Wireless Firewall | A vulnerability exists because DDNS's usernames and passwords are stored in plaintext when a backup of the configuration is made, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| Nylon[69] | Unix | Nylon 0.2 | A remote Denial of Service vulnerability exists because the return value of the recv() call is not properly checked. | Upgrade available at:<br>http://monkey.org/~marius/nylon/nylon-1.0.tar.gz |
| Open Office[70] | Windows, Unix | OpenOffice 1.0.1 | A vulnerability exists in the installation process because temporary files are insecurely created, which could let a malicious user overwrite files and obtain elevated privileges. | No workaround or patch available at time of publishing. |
| Oracle Corporation[71] | Multiple | E-Business Suite 11i 11.1-11.6 | A vulnerability exists in the 'AolSecurityPrivate.class' file because user authentication can be bypassed, which could let a malicious obtain unauthorized access. | Patches available at:<br>http://metalink.oracle.com |

[67] Securiteam October 11, 2002.
[68] Securiteam, October 11, 2002.
[69] Bugtraq, October 10, 2002.
[70] Vapid Labs Advisory, October 11, 2002.
[71] Oracle Security Alert #44, October 4, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Oracle Corporation[72] | Multiple | Oracle 8i Enterprise Edition 8.1.5.1.0, 8.1.5.0.2, 8.1.5.0.0, 8.1.6.1.0, 8.1.6.0.0, 8.1.7.1.0, 8.1.7.0.0, Oracle8i 8.1.5, 8.1.6, 8.1.7.1, 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1 | A Denial of Service vulnerability exists when a malicious user issues the 'SERVICE_CURLOAD' command. | Patches available at:<br>http://metalink.oracle.com |
| Oracle Corporation[73] | Windows | Oracle 9i Application Server 9.0.2 | A Denial of Service vulnerability exists in the Web Cache Manager Tool when a remote malicious user sends a specially formatted HTTP GET request to the Web Cache Administration module. | **Workaround:**<br>Oracle has suggested the workaround of using routers and network firewalls to filt administration ports. Additionally, Oracle has suggested the use of the "Secure Su included with the module. |
| phpBB Group[74] | Multiple | phpBB 2.0.0-2.0.3 | A vulnerability exists in the avatar files due to the naming scheme, which could let a malicious user obtain user's IP addresses. | No workaround or patch available at time of publishing. |
| phpBB mod[75] | Windows, Unix | phpBBmod 1.3.3 | A vulnerability exists in the 'phpinfo.php' sample script, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |
| phpLinkat[76] | Windows, Unix | phpLinkat 0.1 .0 | A Cross-Site Scripting vulnerability exists in the 'showcat.php' script because HTML is not properly filtered from user-supplied input, which could let a malicious user execute arbitrary HTML or script code. | No workaround or patch available at time of publishing. |

[72] Rapid 7, Inc. Security Advisory, R7-0006 , October 9, 2002.
[73] Oracle Security Alert #43, October 4, 2002.
[74] Bugtraq, October 9, 2002.
[75] Bugtraq, October 10, 2002.
[76] Bugtraq, October 3, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| phpRank[77] | Windows, Unix | phpRank 1.8 | Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'add.php' portion of the package, which could let a remote malicious user execute arbitrary code; a vulnerability exists because the Administrator's password is stored plaintext in the source code and in an HTTP cookie called "ap," and all user's passwords are stored in plaintext in the SQL database, which could let a remote malicious user obtain sensitive information; a vulnerability exists when a site is submitted to the banner list because user input is not properly filtered, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because insufficient error checking is provided for functions that access the MySQL database, which could let a remote malicious user obtain unauthorized access. | No workaround or patch available at time of publishing. |
| Polycom[78] | Multiple | ViaVideo 2.2, 3.0 | Several vulnerabilities exist: a Denial of Service vulnerability exists when numerous incomplete HTTP requests are made by a malicious user; and a buffer overflow vulnerability exists when excessively long ET requests are issued, which could let a remote malicious user cause a Denial of Service and possible execute arbitrary code. | Patch available at:<br>http://www.polycom.com/securitycenter |

[77] Bugtraq, October 10, 2002.
[78] Polycom Security Advisory 02-002, October 15, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| RadioBird Software[79] | Multiple | WebServer 4 All 1.23, 4 All 1.27 | Two vulnerabilities exist: a buffer overflow vulnerability exists when an excessively long GET request is issued, which could let a malicious user cause a Denial of Service; and a Directory Traversal vulnerability exists due to inadequate santization when a request is issued that contains hexadecimal representation for the front slash character, which could let a malicious user obtain sensitive information. | Upgrade available at:<br>ftp://ftp.freeware.lt/anonymous/Soft/w4asetup.exe |
| Sabre Inc. [80] | Windows NT | Sabre Desktop Reservation Software 4.4 G | A Denial of Service vulnerability exists when malformed data is sent to the 'Savserv' component. | No workaround or patch available at time of publishing. |
| Script-Shed[81] | Multiple | SSGBook 1.0 | A vulnerability exists because HTML and script code is not properly sanitized from image tags, which could let a malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. |
| Sendmail Consor-tium[82] | Multiple | Sendmail 8.12.6 | Modification was made to the sendmail source code by a malicious user that contains a Trojan horse. Downloads of the sendmail source code from ftp.sendmail.org between September 28, 2002 and October 6, 2002 likely contain the Trojan code.<br>*Note: Versions of sendmail available via HTTP distribution on the Sendmail Consortium site are not affected.* | Valid versions available at:<br>http://www.sendmail.org<br>They are available from the normal distribution channels and have the following M<br>73e18ea78b2386b774963c8472cbd309 sendmail.8.12.6.tar.gz<br>cebe3fa43731b315908f44889d9d2137 sendmail.8.12.6.tar.Z<br>8b9c78122044f4e4744fc447eeafef34 sendmail.8.12.6.tar.sig |

[79] iDEFENSE Security Advisory, 10.15.02, October 15, 2002.
[80] iDEFENSE Security Advisory 10.16.02, October 16, 2002.
[81] Bugtraq, October 8, 2002.
[82] CERT® Advisory CA-2002-28, October 8, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| SGI[83] | Unix | IRIX 6.5-6.5.17, 6.5.13 m- 6.5.17 m | Multiple vulnerabilities exist: a vulnerability exists in the 'rpcbind' utility because symbolic links are incorrectly followed, which could let a malicious corrupt critical system files and possibly cause a Denial of Service or obtain elevated privileges; a vulnerability exists because temporary desktop files are created with world-writable permissions, which could let a malicious user overwrite and corrupt temporary desktop files; a buffer overflow vulnerability exists in the 'uux' binary, which could let a malicious user execute arbitrary code; a vulnerability exists in the 'fsr_efs' binary because symbolic links are incorrectly followed, which could let a malicious user corrupt critical system files and possibly cause a Denial of Service or obtain elevated privileges;  and a vulnerability exists in the 'mv' command because renamed directories are created insecurely, which could let a malicious user overwrite and corrupt critical files on the system. | Upgrades available at:<br>http://www.sgi.com/software/software.html#IRIX<br>Patches available at:<br>ftp://patches.sgi.com/support/free/security/patches |
| Sky Stream Networks[84] | Unix | EMR5000 1.16, 1.17, 1.18 | A remote Denial of Service vulnerability exists because high volumes of traffic are not properly handled in certain situations. | No workaround or patch available at time of publishing. |
| **Squirrel Mail[85]**<br><br>***RedHat issues updated advisory[86]*** | **Unix** | **Squirrel Mail 1.2.7** | **Multiple Cross-Site scripting vulnerabilities exist in various PHP scripts because user input is not properly sanitized, which could let a malicious user execute arbitrary HTML and script code.** | **Upgrade available at:**<br>**http://prdownloads.sf.net/squirrelmail/squirrelmail-1.2.8.tar.gz**<br><br>***Upgrade available at:***<br>**ftp://updates.redhat.com/8.0/en/os/noarch/squirrelmail-1.2.8-1.noarch.rpm** |

[83] SGI Security Advisory, 20020903-01-P, October 14, 2002.

[84] Global InterSec LLC Advisory, 2002021001, October 16, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Squirrel Mail[87] | Unix | Squirrel Mail 1.2.7 | A vulnerability exists in the 'options.php' script when malformed input is provided as arguments, which could let a malicious user obtain sensitive information. | Upgrade available at:<br>http://prdownloads.sf.net/squirrelmail/squirrelmail-1.2.8.tar.gz<br>**RedHat:**<br>ftp://updates.redhat.com/8.0/en/os/noarch/squirrelmail-1.2.8-1.noarch.rpm |
| Sun Microsystems, Inc.[88] | Unix | Solaris 2.5, 2.5.1, 2.5.1_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0 | A Denial of Service vulnerability exists in the 'lockd' daemon if the "lockd" process has been started in debug mode. | Patches available at:<br>Sun Patch 109745-02<br>http://sunsolve.sun.com/pub-cgi/ |
| Surf Control[89] | Windows NT 4.0/2000 | SuperScout E-mail Filter 3.5, 3.5.1, SuperScout E-mail Filter for SMTP 4.0 | Multiple vulnerabilities exist in the e-mail filter in the 'STEMWADM' administrative web interface: a Cross-Site Scripting vulnerability exists because user-supplied input is not filtered, which could let a malicious user execute arbitrary HTML and script code; a vulnerability exists because the 'userlist.asp' file that comes with the web interface contains a listing of administrative usernames/passwords, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists when a malicious user sends a malformed HTTP request that does not contain a Content-Length HTTP Header field; and a Denial of Service vulnerability exists when a malicious user sends an incomplete HTTP GET request that does not contain terminating bytes. | Affected users should contact the vendor about obtaining fixes. |

[85] Bugtraq, September 19, 2002.
[86] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:204-10, October 9, 2002.
[87] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:204-10, October 9, 2002.
[88] Sun(sm) Alert Notification, 47815, October 17, 2002.
[89] Bugtraq, October 9, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| Symantec[90] | Windows NT 4.0/2000, Unix | Enterprise Firewall 6.5.2 NT/2000, 7.0 Solaris, 7.0 NT/2000, Gateway Security 5110, 5200, 5300, Raptor Firewall 6.5 Windows NT, 6.5.3 Solaris, Veloci Raptor 1000, 1100, 1200, 1300, 500, 700 | A remote Denial of Service vulnerability exists in the Web proxy component when a malicious user issues a HTTP-style CONNECT to a domain with a missing, or flawed DNS-server. | Patch available at:<br>http://www.symantec.com/techsupp |
| Symantec[91] | Windows NT 4.0/2000, Unix | Enterprise Firewall 6.5.2 NT/2000, Raptor Firewall 6.5 Windows NT, Raptor Firewall 6.5.3 Solaris | A vulnerability exists in the HTTP proxy because it is possible for external hosts to identify responsive hosts that are connected to the internal interface, which could let a malicious user obtain sensitive information. | Patch available at:<br>http://www.symantec.com/techsupp |
| Symantec[92] | Multiple | Veloci Raptor 1.0, 1.1, 1.5, 1200 , 1300 | A remote Denial of Service vulnerability exists when malformed requests are sent by a malicious user. | Hotfix available at:<br>ftp://ftp.symantec.com/public/updates/security-vr15-3des.zip |
| Symantec[93] | Multiple | Norton AntiVirus Corporate Edition 7.5, 7.6, 7.51 | A vulnerability exists in the 'winhlp32' interface process, which could let a malicious user obtain administrative privileges. | Upgrade information available at:<br>http://securityresponse.symantec.com/avcenter/security/Content/2002.10.15.html |
| Tel Condex Software[94] | Windows NT | SimpleWebServer 2.06 | A remote Denial of Service vulnerability exists because long URL requests are not properly handled. | Upgrade available at:<br>http://www.yourinfosystem.de/download.htm |
| TkMail[95] | Unix | TkMail 4.0 beta9, beta8, beta6, beta4, beta1 | A vulnerability exists because temporary files are handled in an insecure manner, which could let a malicious user overwrite arbitrary files. | Upgrade available at:<br>http://security.debian.org/pool/updates/main/t/tkmail |

[90] Advanced IT-Security Advisory #01-10-2002, October 14, 2002.
[91] Advanced IT-Security Advisory #02-10-2002, October 14, 2002.
[92] SecurityFocus, October 7, 2002.
[93] Symantec Security Advisory, October 15, 2002.
[94] Securiteam, October 15, 2002.
[95] Debian Security Advisory, DSA 172-1, October 8, 2002.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts |
|---|---|---|---|---|
| VBZoom[96] | Windows, Unix | VBZoom 1.0 1 | A vulnerability exists in the 'add-subject.php' script because files are not properly validated, which could let a remote malicious user execute arbitrary commands. | No workaround or patch available at time of publishing. |
| VBZoom[97] | Windows, Unix | VBZoom 1.0 1 | A vulnerability exists due to insufficient sanitization of variables used to construct SQL queries, which could let a remote malicious user execute arbitrary files. | No workaround or patch available at time of publishing. |
| Webmin[98] | Unix | Webmin 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.91-0.990, 1.0 00 | A vulnerability exists because the software is shipped with a built-in SSL key that is the same for every installation, which could let a remote malicious user eavesdrop on or hijack Webmin sessions and possibly decrypt traffic that is sent during the SSL session. | Upgrade available at:<br>http://prdownloads.sourceforge.net/webadmin/webmin-1.020.tar.gz?download |
| Yann Ramin[99] | Unix | ATPhttpd 0.4, 0.4 b | A buffer overflow vulnerability exists when a string with 'count' bytes or more is received by the sock_gets() function, which could let a remote malicious user obtain root access. | No workaround or patch available at time of publishing. |
| Zack Coburn[100] | Unix | Meunity Community System 1.0 | A vulnerability exists because user-supplied script code is not removed from IMG tags, which could let a malicious user execute arbitrary script code. | No workaround or patch available at time of publishing. |
| Zope[101] | Unix | Zope 2.1.1, 2.1.7, 2.2.0, 2.2-2.2.5, 2.3.0-2.3.3, 2.4.0-2.5.1, 2.6.0b1 | A vulnerability exists when the 'Cancel' button is hit after a failed login attempt to the management interface, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. |

*"Risk" is defined by CyberNotes in the following manner:

[96] Bugtraq, October 9, 2002.
[97] Bugtraq, October 8, 2002.
[98] FreeBSD Security Advisory, FreeBSD-SN-02:06, October 10, 2002.
[99] PYR/\MID, Research Project Security Advisory, October 14, 2002.
[100] ECHU Alert #3, October 14, 2002.
[101] Bugtraq, October 7, 2002.

**High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

**Medium** – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

**Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 28 and October 16, 2002, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 27 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| October 16, 2002 | Arp-sk-0.0.15.tgz | An ARP packet generator for Unix designed to illustrate ARP protocol flaws and applications such as ARP cache poisoning and MAC spoofing. |
| October 16, 2002 | Tomcat.dos.sh | Denial of Service exploit for the Apache AUX, LPT1, CON, and PRN vulnerability. |
| October 16, 2002 | Gm011-ie.txt | Exploit HTML for the Internet Explorer Unauthorized DOM<br>Access vulnerability. |
| **October 16, 2002** | **Getad.c** | **Script that exploits the Windows 2000 NetDDE Privilege Escalation vulnerability.** |
| October 15, 2002 | Neuter.c | Remote Denial of Service exploit that can be used against systems running Apache Tomcat (versions prior to 4.1.10) combined with IIS. |
| October 15, 2002 | Prpghttpd.c | Script which exploits the ghttpd Log() Buffer Overflow vulnerability. |
| **October 14, 2002** | **Ingeniumdecoder.java** | **Exploit for the Ingenium Learning Management Weak Algorithm vulnerability.** |
| **October 14, 2002** | **Atphttpd-exp.c** | **Script which exploits the ATP httpd Buffer Overflow vulnerability.** |
| October 9, 2002 | Spike2.7.tar.gz | A web application analysis tool which uses the SPIKE API to help reverse engineer new and unknown network protocols. |
| October 9, 2002 | Sortrace.c | Linux Traceroute v1.4a5 and below local root exploit which takes advantage of a malloc chunk vulnerability. |

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| October 9, 2002 | Mod_ssl-toolkit.tar.gz | Mod_ssl off-by-one vulnerability exploitation toolkit for OpenBSD. |
| **October 9, 2002** | **Euxploit.zip** | **Remote exploit for the Eudora MIME Multipart Boundary Buffer Overflow vulnerability.** |
| October 9, 2002 | Nessus-1.2.6.tar.gz | Uup-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 920 remote security checks. |
| October 9, 2002 | Chmoverflow.zip | Windows Help Buffer Overflow proof of concept remote exploit in Visual Basic 6. |
| October 8, 2002 | Wellenreiter-v16.tar.gz | a GTK/Perl program that makes the discovery and auditing of 802.11b wireless networks much easier. |
| **October 8, 2002** | **Sm.backdoor.base64.txt** | **Exploit for the Sendmail Trojan Horse.** |
| **October 8, 2002** | **Sm.backdoor.patch** | **Exploit for the Sendmail Trojan Horse.** |
| October 6, 2002 | Iosmash2.c | A local root exploit for the FreeBSD file descriptors kernel bug that resides in all releases of FreeBSD up to and including 4.6-RELEASE. |
| October 5, 2002 | Onelove.c | Proof of Concept exploit code that demonstrates how commands can be injected in a ptraced telnet/ssh session. |
| **October 5, 2002** | **Power-ftp-ex.c** | **Script which exploits the PowerFTP Server Remote Denial of Service vulnerability.** |
| **October 5, 2002** | **Ts-pfd.tgz** | **Script which exploits the PowerFTP Server Remote Denial of Service vulnerability.** |
| October 4, 2002 | Tl004.txt | Denial of Service exploit information for the Windows Help Facility vulnerability. |
| **October 4, 2002** | **Bearshare.4.0.6.txt** | **Exploit URL for the BearShare Directory Traversal vulnerability.** |
| **October 4, 2002** | **Telnet.c** | **Script that exploits the Sun Solaris TTYPROMPT Authentication Bypass vulnerability.** |
| October 3, 2002 | Unix/audit/sara/sara-4.1.1.tgz | A security analysis tool based on the SATAN model. It is updated twice a month to address the latest threats. |
| **October 2, 2002** | **Pubappbrute.tar.gz** | **Script which exploits the Citrix Information Disclosure vulnerability.** |
| **September 28, 2002** | **Cinik.tgz** | **A modified version of the Slapper worm that lets the worm mail system information, such as the IP address and processor type, to a Yahoo! e-mail address.** |

## *Trends*

- **The CERT/CC has received confirmation that some copies of the source code for the Sendmail package have been modified by an intruder to contain a Trojan horse. For more information, see "Bugs, Holes, & Patches Table" and CERT® Advisory CA-2002-28 located at: http://www.cert.org/advisories/CA-2002-28.html.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of an e-mail-borne worm known as W32.Bugbear or I-Worm.Tanatos. For more information, see NIPC Advisory 02-008, located at: http://www.nipc.gov/warnings/advisories/2002/02-008.htm and Virus Section.**
- **The National Infrastructure Protection Center (NIPC) has been coordinating with the anti-virus and security community on the life cycle of "Slapper," the OpenSSL/Apache worm and all its variants. For more information, see NIPC ASSESSMENT 02-003, located at: http://www.nipc.gov/warnings/assessments/2002/02-003.htm.**
- **The SANS Institute and the National Infrastructure Protection Center (NIPC) have updated the list containing the Twenty Most Critical Internet Security Vulnerabilities. This list is broken into**

**two categories: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. For more detailed information, see: http://www.sans.org/top20.**

- **A record number of malicious hacking attempts were made during September with more than 4,157 attacks, and anti-American groups are responsible. Systems running Microsoft Windows suffered more attacks than all other operating systems combined, with only 1,740 attacks on Linux, 933 attacks on BSD and 229 attacks on Solaris.**
- **The CERT/CC has received reports of self-propagating malicious code that exploits a known buffer overrun vulnerability in the Secure Sockets Layer 2.0 (SSLv2) handshake process in OpenSSL. This malicious code has been referred to as Apache/mod_ssl worm, linux.slapper.worm, and bugtraq.c worm. For more information see CERT® Advisory CA-2002-27, located at: http://www.cert.org/advisories/CA-2002-27.html. Please ensure that you've applied the appropriate patch.**
- **Statistical weaknesses exist in TCP/IP Initial Sequence Numbers. For more information, see CERT® Advisory CA-2001-09, located at: http://www.cert.org/advisories/CA-2001-09.html.**
- **The Microsoft Product Support Services (PSS) Security Team has issued an alert regarding an increased level of hacking activity. These hacking attempts show similar symptoms and behaviors involving the detection of Trojans such as Backdoor.IRC.Flood and its variants, and the modification of the security policy on domain controllers.**
- **Web CGI exploits and Microsoft vulnerabilities continue to be two of the more frequent ways which external malicious sources conduct their probes in their attempt to gain access to networks.**
- **According to data compiled by its regional Global Command Centers (GCCs), which monitor and protect client networks from cyber-attacks, there has been a surge in cyber-attacks originating from Malaysia over the last quarter. The majority of these attacks were mainly Apache exploit attempts to execute arbitrary codes, which could lead to possible Denial-of-Service (DoS) attacks.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of multiple buffer overflows in OpenSSL (Open Secure Sockets Layer). For more information, see NIPC Advisory 02-006, located at: http://www.nipc.gov/warnings/advisories/2002/02-006.htm.**

# *Viruses*

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

**VBS.Chick.H@mm (Aliases: I-Worm.Brit.h, VBS/Chick.h@M) (Visual Basic Script Worm):** This is a minor variant of VBS.Chick@mm that uses Microsoft Outlook to distribute itself via e-mail. The e-mail would arrive with the subject "RE: Jeniffer Lopez" and an attachment of "Jennifer.chm."

**VBS.Indra.B@mm (Visual Basic Script Worm):** This is a worm that uses Microsoft Outlook to send itself to all contacts in the Microsoft Outlook Address book. When VBS.Indra.B@mm runs, it searches for the value, "Hitschicker2002_sent," in registry key:

- HKEY_CURRENT_USER\Software

If the value exists and the value data is yea, the worm quits without doing anything. Otherwise, the worm uses Microsoft Outlook to send itself to all contacts in the Outlook Address Book. The e-mail message has the following characteristics:

- Subject: World-Trade-Center
- Attachment: The attachment name varies.

The worm then adds the value, "Hitschicker2002_sent yea," to the registry key:

- HKEY_CURRENT_USER\Software

**WORM_HOBBIT.G (Alias: W32/Hobbit.c@MM) (Win32 Worm):** This Win32 worm propagates via Microsoft Outlook as well as the KaZaA network. In Microsoft Outlook, it sends itself as an e-mail message with the following details:

- Subject: Fwd: Scan your computer for this new virus threat...
- Message Body: This is a fix and removal for the new Internet worm known as BugBear. 1 in ever 4 computers in infected with this virus. When run, it will scan your computer and notify you if you're infected or not, then clean if infected.
- Attachment: Anti-Bug.exe

To make itself easily accessible over the KaZaA network, this worm copies itself to the following folders:

- C:\KaZaa\My Shared Folders
- C:\Program Files\KaZaa\My Shared Folders

**W32/Appix-B (Aliases: I-Worm.Apbost, W32/Xiv.b virus) (Win 32 Virus):** This is a virus that arrives in an e-mail with the various subject lines and attached files. The virus attempts to exploit a MIME Vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double clicking on the attachment. When the virus is executed, it creates a copy of itself in the Windows folder called Appboost.exe and changes the registry by setting the following entry to point to Appboost.exe so that this file will be executed every time an EXE file is run:

- HKLM\Software\Classes\exefile\shell\open\command

W32/Appix-B attempts to stop the multiple services. This virus may also infect PHP and PHTML files by adding code that is intended to spread via PHP, PHTML, HTM, and HTML files. Microsoft has issued a patch that secures against the incorrect MIME header vulnerability that can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-027.asp. (This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this virus.)

**W32/Cazinat.worm.b (Win32 Worm):** This is an intended mass-mailer and KaZaA worm. The virus contains bugs in the code and does not propagate as intended. It attempts to e-mail random addresses in the domains TIN.IT, HOTMAIL.COM, YAHOO.IT, and INWIND.IT and MSN Messenger contacts. When the attachment is run, the worm gathers e-mail addresses on the MSN Messenger contact list. These addresses are stored in the %TEMP% directory in the file Contact-e-mail.ini. The worm contacts the server smtp.aruba.it for sending. However, the propagation routine does not succeed as the worm attaches the file c:\windows\system\Figura.scr. The following registry key value is created:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ "Veline" = Veline.exe

**W32/Gaga.worm (Win32 Worm):** This virus is written in Visual Basic 6.0 and spreads by copying itself to floppy discs as NUDEBABES.SCR. Additionally, it attempts to deliver a destructive file deletion payload. When run on the victim machine, it copies itself to %WinDir% as GAGO.EXE the following Registry key is set to run the virus at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
  Run "Aileen Picture" = %WinDir%\GAGO.EXE

and a graphic is displayed. Subsequently, the file deletion payload is delivered. The virus attempts to delete all files on the local hard drive.

**W32.HLLC.Samand (Alias: W32.HLLO.Samand) (Win32 Worm):** This is a companion virus that overwrites one .exe file in the current folder. It contains no damaging payload and no spreading mechanism.

**W32.HLLW.Shorm.B (Alias: W32/Shorm.worm.gen) (Win32 Worm):** This is a 32-bit worm that spreads by attempting to connect to a predetermined set of IP addresses. It contains a password stealer. The worm e-mails passwords to the malicious user using an anonymous mail host in Russia. It is a variant of W32.HLLW.Shorm. Because it updates itself when it runs, the names of the files that it drops are not constant. When the worm starts, it checks a Web site in Russia for updated versions, which are usually named Wormxx.bmp, where xx is a two-digit value. The worm downloads the new file and runs it. When the file runs, the worm moves itself to the %windir% folder. Known file names to which the worm moves itself are:

Interet32.exe
Winint32.exe

The worm also changes registry settings. If the dropped file is %windir%\Interet32.exe, it adds the value, “Interet32 Interet32.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

If the dropped file is %windir%\Winint32.exe, it adds the value, “Winint32 Winint32.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

If the dropped file is %windir%\Files32.vxd, it changes the (Default) value of :

- HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command

to Files32.vxd "%1%” This causes the worm to run whenever an .exe file runs. The worm also downloads a file containing the first three octets of an IP address range. It then tries to connect to the addresses by filling in the last octet. It tests for shares and attempts to copy itself into the Windows startup folder. It copies itself as one of the following:

- Auto.exe
- Auto16.exe
- Worm23.exe
- Worm25.exe
- Script.exe

By placing itself into this folder, the worm runs each time that you start Windows.

**W32.Lamecada@mm (Win32 Worm):** This is a mass-mailing worm that sends itself to all contacts in the Microsoft Outlook Address Book. The worm can spread only by using Microsoft Outlook. W32.Lamecada@mm is a worm that is written in Visual Basic 6.0. If you W32.Lamecada@mm is executed, it creates the following copies of itself:

- %windir%\W32.worm.calamida.exe
- %windir%\Setup.exe
- %system%\3Dfx.dll

The worm also accesses the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

and changes the (Default) value to, “%Windows%\W32.WORM.CALAMIDA.exe” so that the worm runs each time that you start Windows. It inventories your Microsoft Outlook Address Book, and sends e-mail to all contacts, using this format:

- Subject: Internet Explorer Bugs Fix Setup
- Message body: Please run this setup to fix some problem your Internet Explorer Browser. Open the file : setup.exe

Attachment: Setup.exe

**W32/Rodok-A (Aliases: BR2002, W32.HLLW.Henpeck, W32/Fleming.worm, Win32.Fleming.A, Worm.Win32.Fleming) (Win32 Worm):** This is a worm that spreads via MSN Messenger and sends the message:

- "Hey!! Could you please check out this program for me? :) I made it myself and want people to test it. It’s a readme with the program that explains what it does! http://home.no.net/downl0ad/BR2002.exe <-- There you can download it! give me advice on what to upgrade please!!"

The worm also attempts to download and execute Troj/Brat from the web site described in the message. Afterwards, the worm displays a fake CD key generator. W32/Rodok-A is also capable of stealing keys for the games Half-Life and Counter-Strike and sending them to a Hotmail e-mail address.

**Worm/PackagerFX (Internet Worm):** This is an Internet worm that targets the KaZaA file-sharing network. If executed, the worm pops open a fake antivirus software windows. As it is performing this fake scan, it copies itself in the \windows\ directory under the filename "IrRMFoXJyG.exe (random file name).” So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run __IqRMFoXJyG"="C:\\WINDOWS\\IqRMFoXJyG.exe

In order to make itself available through the KaZaA network, the following registry modifications are added:

- HKEY_CURRENT_USER\Software\KAZAA\LocalContent "BehindProxy"="1" "KaZaARegKey"="IqRMFoXJyG" “DisableSharing"="0"

After the worm installs itself, another fake window will open with a message for rebooting the system. If the user chooses "Ok" then the system will be restarted re-initializing the worm. Because the keyboard is blocked, sooner or later the user will be required to press the OK button of the fake window.

**WORM_PAKGER.A (Aliases: PAKGER.A, W32/Tufast.worm) (Win32 Worm):** This worm propagates by copying itself to the KaZaA shared folder. It also attempts to connect to an IRC (Internet Relay Chat) server, possibly to inform the author that the infected user is online. Upon execution, this worm displays a message box, which is designed to trick the target user into thinking that this program is a worm remover, similar to an antivirus program. he message box has the following text strings:

- AVP-Antiviral Toolkit Pro
- Drive to scan and clean PackAger I-Worm
- AVP is NOT FREE/SHAREWARE
- You have to register AVP for new benefits
- This software will run once on this computer.
- ready to scan..

This message box has a SCAN NOW button, which simulates a scanning process when clicked. It displays another message box to let the unsuspecting user think that it is indeed scanning. What actually happens behind this "scanning process" is the installation of the worm on the target system. After it has finished "scanning and cleaning" the system, this worm then asks the target user to restart the machine. It displays another message box with the following text strings:

- AVP-Antiviral Toolkit Pro
- Rebooting now to finish the disinfection

When the target user closes this message box by clicking the x button, this worm installs itself on the system. It drops a copy of itself in the Windows directory with a random filename. To enable its automatic execution every system startup, this worm modifies the registry by creating an autorun registry entry. The modified registry appears as follows:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run <name1> = %Windows%\<name1>.exe

It also adds the following registry entries to enable its propagation over the KaZaa network:

- HKEY_CURRENT_USER\Software\KAZAA\LocalContent BehindProxy="1"
- HKEY_CURRENT_USER\Software\KAZAA\LocalContent KaZaARegKey="<name1>"
- HKEY_CURRENT_USER\Software\KAZAA\LocalContent DisableSharing="0"

This worm propagates by copying itself to the KaZaA shared folder. To do this, it gets the filename of an existing non-executable file on the said folder and then creates a copy of itself using the said filename but with an EXE extension. This worm also attempts to connect an IRC server, possibly to inform its author that the infected user is online.

**Worm/Walrus (Alias: IRC-Worm.Freep) (IRC Worm):** This is an Internet worm that spreads via the Internet Rely Chat (IRC) network. If executed, the worm copies itself in the C:\ directory under the filename "FreePorn.com.” The files "C:\Mirc\Script.ini" and "C:\Program Files\Mirc\Script.ini" get created. It will also attempt to appear legitimate by popping open an explicit image.

**Worm/Zetno (Internet Worm):** When Worm/Zetno is executed, the worm copies itself in the \windows\ directory under the filename "Winsysger.exe" (1.025 Kbytes). Additionally, the files "C:\Zetno.exe (11.541 Kbytes)" and "C:\Windows\System\Zipload32.exe (11.541 Kbytes)" are created new. The following modifications are done to the various files:

- C:\Windows\System.ini
  shell=Explorer.exe
  shell=Explorer.exe Zipload32.exe
- C:\Windows\Win.ini

  run=
  run=Zipload32.exe

- C:\Windows\Win.ini
  load=
  load=Zipload32.exe

**XM97/Divi-AC (Excel 97 Macro Virus):** This virus has been reported in the wild. It is a member of the XM97/Divi Excel macro virus family. XM97/Divi-AC creates an infectious file named 874.xls in the XLSTART directory.

## *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| AIM-Flood | N/A | CyberNotes-2002-16 |
| Arial | N/A | CyberNotes-2002-08 |
| **Backdoor.AIMVision** | **N/A** | **Current Issue** |
| Backdoor.Anakha | N/A | CyberNotes-2002-13 |
| Backdoor.AntiLam | N/A | CyberNotes-2002-12 |
| Backdoor.AntiLam.20 | 20 | CyberNotes-2002-18 |
| Backdoor.Armageddon.B | N/A | CyberNotes-2002-20 |
| **Backdoor.Asniffer** | **N/A** | **Current Issue** |
| Backdoor.Assasin | N/A | CyberNotes-2002-14 |
| Backdoor.Cabro | N/A | CyberNotes-2002-17 |
| Backdoor.Cabrotor | N/A | CyberNotes-2002-18 |
| Backdoor.Crat | N/A | CyberNotes-2002-12 |
| Backdoor.Cyn | N/A | CyberNotes-2002-18 |
| Backdoor.DarkFtp | N/A | CyberNotes-2002-19 |
| Backdoor.DarkSky.B | B | CyberNotes-2002-20 |
| **Backdoor.DarkSky.C** | **C** | **Current Issue** |
| Backdoor.Delf | N/A | CyberNotes-2002-16 |
| Backdoor.Delf.B | B | CyberNotes-2002-16 |
| Backdoor.Delf.C | C | CyberNotes-2002-17 |
| Backdoor.Ducktoy | N/A | CyberNotes-2002-15 |
| Backdoor.Easyserv | N/A | CyberNotes-2002-16 |
| Backdoor.Elitem | N/A | CyberNotes-2002-20 |
| Backdoor.Evilbot | N/A | CyberNotes-2002-09 |
| Backdoor.Expjan | N/A | CyberNotes-2002-18 |
| **Backdoor.Feardoor** | **N/A** | **Current Issue** |
| Backdoor.Fearic | N/A | CyberNotes-2002-16 |
| Backdoor.FTP_Ana | N/A | CyberNotes-2002-20 |
| Backdoor.FTP_Ana.B | B | CyberNotes-2002-20 |
| Backdoor.FTP_Bmail | N/A | CyberNotes-2002-12 |
| Backdoor.FunFactory | N/A | CyberNotes-2002-19 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Backdoor.Goster | N/A | CyberNotes-2002-20 |
| Backdoor.GRM | N/A | CyberNotes-2002-13 |
| Backdoor.GSpot | N/A | CyberNotes-2002-12 |
| **Backdoor.GWGhost** | **N/A** | **Current Issue** |
| Backdoor.Helios | N/A | CyberNotes-2002-19 |
| **Backdoor.Hupigeon** | **N/A** | **Current Issue** |
| Backdoor.Kaitex.B | N/A | CyberNotes-2002-20 |
| Backdoor.Kavar | N/A | CyberNotes-2002-16 |
| Backdoor.Kryost | N/A | CyberNotes-2002-18 |
| Backdoor.Laphex | N/A | CyberNotes-2002-18 |
| Backdoor.Laphex.Client | N/A | CyberNotes-2002-18 |
| Backdoor.Lastdoor | N/A | CyberNotes-2002-18 |
| Backdoor.Latinus | N/A | CyberNotes-2002-12 |
| Backdoor.Latinus.B | B | CyberNotes-2002-18 |
| Backdoor.Litmus.2a | 2a | CyberNotes-2002-20 |
| Backdoor.Miffice | N/A | CyberNotes-2002-18 |
| Backdoor.Mirab | N/A | CyberNotes-2002-13 |
| Backdoor.Mite | N/A | CyberNotes-2002-18 |
| Backdoor.MLink | N/A | CyberNotes-2002-16 |
| Backdoor.Ndad | N/A | CyberNotes-2002-17 |
| Backdoor.NetControle | N/A | CyberNotes-2002-13 |
| Backdoor.Nota | N/A | CyberNotes-2002-12 |
| Backdoor.Omed.B | B | CyberNotes-2002-11 |
| Backdoor.Optix.04 | 04 | CyberNotes-2002-19 |
| Backdoor.OptixPro.10 | 10 | CyberNotes-2002-18 |
| Backdoor.OptixPro.11 | 11 | CyberNotes-2002-20 |
| Backdoor.OptixPro.12 | 12 | CyberNotes-2002-18 |
| Backdoor.Osirdoor | N/A | CyberNotes-2002-17 |
| Backdoor.Pest.Cli | N/A | CyberNotes-2002-20 |
| Backdoor.Pestdoor | N/A | CyberNotes-2002-20 |
| Backdoor.Phoenix | N/A | CyberNotes-2002-19 |
| **Backdoor.Platrash** | **N/A** | **Current Issue** |
| Backdoor.Ptakks.B | N/A | CyberNotes-2002-18 |
| Backdoor.RCServ | N/A | CyberNotes-2002-19 |
| Backdoor.RemoteNC | N/A | CyberNotes-2002-09 |
| Backdoor.RMFDoor.Cli | N/A | CyberNotes-2002-20 |
| Backdoor.Robi | N/A | CyberNotes-2002-18 |
| Backdoor.Roxrat.10 | N/A | CyberNotes-2002-20 |
| Backdoor.Sazo | N/A | CyberNotes-2002-13 |
| Backdoor.Scanboot | N/A | CyberNotes-2002-17 |
| Backdoor.Seamy | N/A | CyberNotes-2002-18 |
| Backdoor.Sparta | N/A | CyberNotes-2002-13 |
| Backdoor.Sparta.B | B | CyberNotes-2002-19 |
| **Backdoor.Sparta.C** | **C** | **Current Issue** |
| Backdoor.Tela | N/A | CyberNotes-2002-17 |
| Backdoor.Theef | N/A | CyberNotes-2002-15 |
| **Backdoor.Theef.B** | **B** | **Current Issue** |
| Backdoor.Tron | N/A | CyberNotes-2002-12 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Backdoor.Ultor | N/A | CyberNotes-2002-13 |
| Backdoor.WinShell | N/A | CyberNotes-2002-16 |
| Backdoor.Y3KRat.15 | N/A | CyberNotes-2002-17 |
| Backdoor.Zenmaster | N/A | CyberNotes-2002-19 |
| Backdoor-AKO | N/A | CyberNotes-2002-20 |
| BackDoor-AKR | N/A | CyberNotes-2002-19 |
| **BackDoor-ALT** | **N/A** | **Current Issue** |
| Banan.Trojan | N/A | CyberNotes-2002-15 |
| Bck/Litmus.201 | N/A | CyberNotes-2002-14 |
| BDS/ConLoader | N/A | CyberNotes-2002-12 |
| BDS/EHKSLogger | N/A | CyberNotes-2002-19 |
| BDS/Pestdoor.4 | N/A | CyberNotes-2002-20 |
| BDS/Sporkbot | N/A | CyberNotes-2002-20 |
| BKDR_EMULBOX.A | N/A | CyberNotes-2002-10 |
| BKDR_INTRUZZO.A | N/A | CyberNotes-2002-09 |
| BKDR_LITMUS.C | N/A | CyberNotes-2002-09 |
| Bneo.Trojan | N/A | CyberNotes-2002-18 |
| Cardst | N/A | CyberNotes-2002-17 |
| Cytron | N/A | CyberNotes-2002-20 |
| Dewin | N/A | CyberNotes-2002-08 |
| Downloader-W | N/A | CyberNotes-2002-08 |
| FakeGina.Trojan | N/A | CyberNotes-2002-16 |
| Fortnight | N/A | CyberNotes-2002-10 |
| IIS.Beavuh-Exploit | N/A | CyberNotes-2002-17 |
| IRC.kierz | N/A | CyberNotes-2002-16 |
| IRC-Smev | N/A | CyberNotes-2002-08 |
| Jekord | N/A | CyberNotes-2002-19 |
| JS/NoClose | N/A | CyberNotes-2002-11 |
| Liquid.Trojan | N/A | CyberNotes-2002-14 |
| mIRC/Gif | N/A | CyberNotes-2002-08 |
| Multidropper-CX | N/A | CyberNotes-2002-08 |
| Netbus.160.Dropper | N/A | CyberNotes-2002-17 |
| PWS-AOLFake | N/A | CyberNotes-2002-15 |
| PWS-MSNCrack | N/A | CyberNotes-2002-18 |
| PWS-MSNSteal | N/A | CyberNotes-2002-17 |
| PWS-Ritter | N/A | CyberNotes-2002-16 |
| PWSteal.BStroj | N/A | CyberNotes-2002-20 |
| PWSteal.Kaylo | N/A | CyberNotes-2002-17 |
| PWSteal.Netsnake | N/A | CyberNotes-2002-17 |
| PWSteal.Profman | N/A | CyberNotes-2002-17 |
| PWSteal.SoapSpy | N/A | CyberNotes-2002-18 |
| QDel227 | N/A | CyberNotes-2002-09 |
| QDel234 | N/A | CyberNotes-2002-11 |
| RCServ | N/A | CyberNotes-2002-10 |
| Reboot-R | N/A | CyberNotes-2002-18 |
| StartPage-B | N/A | CyberNotes-2002-16 |
| Swporta.Trojan | N/A | CyberNotes-2002-13 |
| TR/EvilDX | N/A | CyberNotes-2002-19 |
| TR/Win32.Rewin | N/A | CyberNotes-2002-12 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Tr/WiNet | N/A | CyberNotes-2002-10 |
| TR/WLoader | N/A | CyberNotes-2002-20 |
| TR/Zirko | N/A | CyberNotes-2002-10 |
| Trj/GhostGirl | N/A | CyberNotes-2002-19 |
| Troj/Apher-A | N/A | CyberNotes-2002-17 |
| Troj/Diablo | N/A | CyberNotes-2002-09 |
| Troj/DSS-A | N/A | CyberNotes-2002-12 |
| Troj/FireAnv-A | N/A | CyberNotes-2002-19 |
| Troj/Flood-O | N/A | CyberNotes-2002-14 |
| Troj/Kbman | N/A | CyberNotes-2002-10 |
| Troj/Momma-B | N/A | CyberNotes-2002-11 |
| **Troj/Netdex-A** | **N/A** | **Current Issue** |
| Troj/Ritter-A | N/A | CyberNotes-2002-17 |
| Troj/Tobizan-A | N/A | CyberNotes-2002-16 |
| Troj/Unreal-A | N/A | CyberNotes-2002-16 |
| TROJ_DOAL.A | N/A | CyberNotes-2002-14 |
| TROJ_JUNTADOR.G | N/A | CyberNotes-2002-10 |
| TROJ_OPENME.B | N/A | CyberNotes-2002-09 |
| TROJ_SMALL.J | N/A | CyberNotes-2002-10 |
| TROJ_SMBNUKE.A | N/A | CyberNotes-2002-18 |
| TROJ_SQLSPIDA.B | N/A | CyberNotes-2002-11 |
| TROJ_SUOMIA.A | N/A | CyberNotes-2002-18 |
| TROJ_WORTRON.10B | N/A | CyberNotes-2002-12 |
| Trojan.Adclicker | N/A | CyberNotes-2002-19 |
| Trojan.Adnap | N/A | CyberNotes-2002-17 |
| Trojan.Allclicks.A | N/A | CyberNotes-2002-13 |
| Trojan.Avid | N/A | CyberNotes-2002-19 |
| Trojan.Beway | N/A | CyberNotes-2002-15 |
| Trojan.Crabox | N/A | CyberNotes-2002-17 |
| Trojan.DiabKey | N/A | CyberNotes-2002-18 |
| Trojan.Diskfil | N/A | CyberNotes-2002-19 |
| Trojan.Fatkill | N/A | CyberNotes-2002-09 |
| Trojan.IrcBounce | N/A | CyberNotes-2002-19 |
| Trojan.Junnan | N/A | CyberNotes-2002-16 |
| Trojan.Lovead | N/A | CyberNotes-2002-19 |
| Trojan.Nullbot | N/A | CyberNotes-2002-19 |
| Trojan.Portacopo:br | N/A | CyberNotes-2002-16 |
| Trojan.Prova | N/A | CyberNotes-2002-10 |
| Trojan.PSW.Ajim_bbs | N/A | CyberNotes-2002-19 |
| Trojan.PSW.CrazyBilets | N/A | CyberNotes-2002-12 |
| Trojan.PSW.M2 | N/A | CyberNotes-2002-13 |
| **Trojan.PWS.QQPass.C** | **N/A** | **Current Issue** |
| Trojan.Starfi | N/A | CyberNotes-2002-16 |
| Trojan.Win32.Filecoder | N/A | CyberNotes-2002-18 |
| Trojan.Win32.MSNTrick | N/A | CyberNotes-2002-17 |
| Trojan.WinReboot | N/A | CyberNotes-2002-20 |
| **UNIX_ALUTAPS.A** | **N/A** | **Current Issue** |
| VBS.Lavra.B.Worm | N/A | CyberNotes-2002-19 |
| VBS.Zevach | N/A | CyberNotes-2002-15 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| VBS_CHICK.B | N/A | CyberNotes-2002-07 |
| W32.Azak | N/A | CyberNotes-2002-16 |
| W32.Cbomb | N/A | CyberNotes-2002-16 |
| W32.Click | N/A | CyberNotes-2002-15 |
| W32.DSS.Trojan | N/A | CyberNotes-2002-09 |
| W32.Estrella | N/A | CyberNotes-2002-13 |
| W32.Evala.Worm | N/A | CyberNotes-2002-14 |
| W32.IRCBot | N/A | CyberNotes-2002-14 |
| W32.Kamil | N/A | CyberNotes-2002-16 |
| W32.Kotef | N/A | CyberNotes-2002-16 |
| W32.Libi | N/A | CyberNotes-2002-10 |
| W32.Maldal.J | N/A | CyberNotes-2002-07 |
| W32.Nuker.Winskill | N/A | CyberNotes-2002-15 |
| W32.Tendoolf | N/A | CyberNotes-2002-09 |
| W32.Wabbin | N/A | CyberNotes-2002-15 |
| WbeCheck | N/A | CyberNotes-2002-09 |
| Winshell | N/A | CyberNotes-2002-15 |
| Worm/Garra | N/A | CyberNotes-2002-20 |

**Backdoor.AIMVision (Alias: Backdoor.AIMVision.12):** This is a Trojan horse that allows unauthorized access to an infected computer. The Trojan is written in Microsoft Visual Basic version 6 and is packed with UPX. When the Trojan runs, it copies itself as %windir%\%system%\qI00tbz.exe. It adds the value, “bbbbb      %windir%\%system%\qI00tbz.exe,” to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It modifies the value, “(Default) %windir%\%system%\qI00tbz.exe %1 %*,” in the registry key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command

so that the Trojan runs when you run an .exe file. The Trojan notifies the client side by using ICQ pager. After Backdoor.AIMVision is installed, it opens port 1111 and waits for commands from the remote client. If a connection is established by a malicious user, the malicious user can steal AOL Instant Messenger (AIM) passwords and configurations and control AIM.

**BackDoor-ALT:** This is a remote access Trojan, which was installed upon visiting a website. The backdoor allows a remote attacker to perform various functions such as run programs, display alert messages, send e-mail, update Trojan, sleep, etc. The website in question was shutdown shortly after the Trojan was discovered. Upon visiting an infectious website, a page is loaded that exploits the "Microsoft VM ActiveX Component" Vulnerability. Several files are written to the COOKIES folder and run.

**Backdoor.Asniffer (Alias: Backdoor.Asniffer.03):** This is a backdoor Trojan horse that opens a port on the computer, allowing a malicious user to remotely access the computer. It can capture packets and log them. The Trojan is written in the Delphi programming language. There are two variants of the Trojan. Both variants can capture packets. To do this, Packet.dll must be installed on the computer.
**Variant 1:** This is 473,088 bytes in size. If it is run, it copies itself as %system%\Explorer.exe. It adds the value, “Explorer      %system%\Explorer.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows. It opens port 8090.
**Variant 2:** This is 492,032 bytes in size. If it is run, it copies itself as %system%\Explorer.exe. It adds the value, “Packet001      \%system%\packet001.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows. It opens port 21217.

**Backdoor.DarkSky.C:** This is a Trojan that is used to gain unauthorized access to an infected computer. It copies itself to the %windir% and %system% folders. When the Trojan is executed, it first runs as a service and then copies itself as:

- %system%\Msinter.exe
- %system%\Notepd.exe
- %windir%\Mobbs.exe
- %windir%\Nuscr.exe

This Trojan then adds the value, "askMonitor %windir%\%system%\Msinter.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time that you start Windows. In the registry key:

- HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command

it changes the (Default) value to, "%windir%\%system%\Notepd.exe "%1" %*," so that the Trojan runs each time that you run an .exe file. In the registry key:

- HKEY_CLASSES_ROOT\txtfile\shell\open\command

it changes the (Default) value to, "%windir%\%system%\Notepd.exe "%1"," so that the Trojan runs each time that you open a .txt file. In the registry key:

- HKEY_CLASSES_ROOT\scrfile\shell\open\command

it changes the (Default) value to, "%windir%\Nuscr.exe "%1"," so that the Trojan runs each time that you run a .scr file. In the registry key:

- HKEY_CLASSES_ROOT\chm.file\shell\open\command

it changes the (Default) value to, "%windir%\Nuscr.exe "%1"," so that the Trojan runs each time that you open .chm (Help) file. The Trojan also adds the line run=%windir%\Mobbs.exe in the Win.ini file. This will run the Trojan each time that you start Windows on Windows 95/98/ME computers.

**Backdoor.Feardoor (Alias: Backdoor.Feardoor.161):** This is a backdoor Trojan that allows a malicious user to remotely control an infected computer. It is written in the Microsoft Visual Basic version 6 programming language. The backdoor opens four ports by default: 1218, 1219, 2000, and 6697. When Backdoor.Feardoor runs, it copies itself as \Windows\System32\Directx\DxDiag.exe. This path is hard-coded, and the file is not copied if the path and folder structure does not exist. The Trojan adds these lines:

- load=\Windows\System32\Directx\DxDiag.exe
- open=\Windows\System32\Directx\DxDiag.exe

to the Win.ini file and the line, "\Windows\System32\Directx\DxDiag.exe," to the Autoexec.bat file. As a result, on Windows 95/98/Me-based computers, the Trojan runs each time that you start Windows. The Trojan drops Visual Basic runtime libraries (such as Mswinsck.ocx and Msinet.ocx) into the %system% folder.

**Backdoor.GWGhost (Alias: Trojan.Spy.GWGhost):** This is the server portion of a backdoor Trojan and is accessible from several know Trojan clients. It allows unauthorized access to the infected computer. When Backdoor.GWGhost runs, it copies itself as %windir%\System\Scanregw.exe. It also creates a file named "%windir%\System\DXInput.dll." The Trojan configures the system to allow it to run; it does so by modifying (or adding) the value, "ScanRegistry %windir%\system\scanregw.exe /autorun," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Users of Norton Registry Tracker should be aware that there is a legitimate Scanregw.exe in the %windir% folder (not the \System folder), and that the registry value for ScanRegistry should point to %windir%\Scanregw.exe.

**Backdoor.Hupigeon:** This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. It is written using the Delphi programming language and packed with UPX. When Backdoor.Hupigeon runs, it copies itself as:

- %system%\Winndow386.exe
- %windows%\N0tepad.exe

It creates the value, "winndow386 %system%\Winndow386.exe," in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. It modifies the value, "(Default) %windows%\N0tepad.exe %1," in the registry keys:

- HKEY_CLASSES_ROOT\txtfile\shell\open\command
- HKEY_CLASSES_ROOT\inifile\shell\open\command

It modifies the value, "(Default) %system%\Winndow386.exe %1 %*," in the registry key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command

As a result of these modifications, the Trojan will start anytime that you open a .txt file, or run a exe or .ini file. The Trojan allows the malicious user to do any of the following:

- Enable/disable the Trojan
- Open/close CD-ROM drive
- Steal ICQ configurations
- Steal system information
- Log keystrokes

**Backdoor.Platrash:** This is a Trojan horse that can allow unauthorized access to an infected computer. The Trojan is written in Microsoft Visual Basic version 6. The original name of the Trojan is Net.exe, but it is not a fixed name, so it can be changed to any file name. When the Trojan runs, it copies itself as %windir%\%system%\<executed file>.exe. It adds the value, "<executed file> <executed file>.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs when you start Windows. The Trojan notifies the client side by using ICQ pager. After Backdoor.Platrash is installed, it opens ports 23005 and 23006 and waits for commands from the remote client. If a connection is established by a malicious user, he or she can do any of the following:

- Download and upload files
- Delete files
- Execute files
- Restart Windows
- Close Windows
- Display messages
- Open/close the CD-ROM tray
- Log keystrokes

**Backdoor.Sparta.C (Alias: Backdoor.Spartadoor.11):** This is a backdoor Trojan horse that opens a port on the computer, allowing a malicious user to remotely access the computer. The Trojan also sends a message to the malicious user with IP address information. Furthermore, it attempts to kill the processes and delete the files of several personal firewall and antivirus products.

**Backdoor.Theef.B (Alias: Backdoor.Theefle.10):** This is a Trojan that can allow unauthorized access to an infected computer. It opens port 9871 to listen for a connection. The Trojan is written in Delphi. If a connection is established by a malicious user, it will be possible for the malicious user to remotely access your system and do any of the following:

- Download and upload files
- Install customized plug-ins for the Trojan
- Delete files
- Execute files
- Restart Windows
- Close Windows
- Display messages

The Trojan copies itself as %windir%\%system%\Genv.exe. It adds the value, "AutoUpdate %windir%\%system%\Genv.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

so that it runs when you start Windows.

**Troj/Netdex-A:** This is a backdoor Trojan that allows unauthorized remote access to the computer. The Trojan is composed of several parts. When a user connects to an infected website, the file BANNER.HTML may be run. BANNER.HTML drops and executes two files on the victim's computer, A.COM and ZSHELL.JS. ZSHELL.JS is dropped in the Cookies folder. When this file is run it drops a BAT file to execute and delete A.COM. The BAT file is then also deleted. Finally ZSHELL.JS runs NETD.EXE which is created in the Windows Temp folder when A.COM is run. All communication to the remote server goes through NETD.EXE, which downloads the file INSTALL.PHP from the remote server. INSTALL.PHP creates the file REPOST.HTML and edits a registry entry to point to this file. It then runs NETD.EXE with a parameter to get SH.PHP. SH.PHP is the main Trojan script and runs NETD.EXE with an option to retrieve the set of commands that the Trojan should execute. SH.PHP is then copied over ZSHELL.JS (NETD.EXE uses two files for input and output: it reads I.JS for input to send to the server and it writes the received data to O.JS. The new O.JS is copied over the old ZSHELL.JS to enable remote updating). The time zone synchronization registry entries are modified to point to ZSHELL.JS so that it is periodically run.

**Trojan.PWS.QQPass.C (Alias: Trojan.PWS.QQPass.gKb6):** This is a password-stealing Trojan. It steals passwords and user information. It is a Visual Basic application that requires the presence of Microsoft Visual Basic runtime libraries for it to run. When it is executed, it searches for and tries to terminate any processes that match the following names:

- Kav9x.exe
- Smenu.exe
- Ravmon.exe

It renames %windir%\Notepad.exe to %windir%\Mspad.exe and then copies itself as these files:

- %windir%\Eudcedit.exe
- %windir%\Freecell.exe
- %windir%\Kaedit.exe
- %windir%\Msscr.exe
- %windir%\Notepad.exe
- %system%\Mstray.exe

This modifications to the system cause the Trojan to be launched each time that a text file that is associated with Notepad is opened. Trojan.PWS.QQPass.C then launches Mspad.exe (which is the original Notepad.exe). Trojan.PWS.QQPass.C then hooks the system by creating registry values (and keys as needed): It adds the value, "SystemKav %system%\MSTRAY.EXE," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

It changes the (Default) value of:

- HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\regfile\shell\open\command

to, "(Default) %windir%\KAEDIT.EXE %1" It changes the (Default) value of:

- HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\scrfile\shell\open\command

to, "(Default) %windir%\MSSCR.EXE %1." It changes the (Default) value of:

- HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\chm.file\shell\open\command

to, "(Default) %windir%\MSSCR.EXE %1." These registry changes cause Trojan.PWS.QQPass.C to be executed when:

- The system is restarted
- A registry file is opened
- A screen saver is executed
- A compiled Help file is opened.

In its resourcesTrojan.PWS.QQPass.C contains these strings:

- FileDescription: Task Monitor
- InternalName: Winpad
- OriginalName: Winpad.EXE

**UNIX_ALUTAPS.A (Aliases: Unix/Sendmail-ADM, Unix/Backdoor-ADM):** This malware is a Trojanized version of Sendmail 8.12.6 that compromises security on affected UNIX systems. This backdoor malware compromises security on affected systems. It is contained in the malicious user modified file, /libsm/t-shm.c, of the Sendmail 8.12.6 package. Once a user builds the package and runs the sendmail program, this malware is extracted from the Trojanized file. This backdoor malware connects to an IP address via TCP port 6667 and then waits for instructions from its remote user. It allows the user to open a remote shell that runs in the context of the affected system. It grants the remote user the same access rights as the regular user of the compromised system.